

1 WO
2
3
4

5 UNITED STATES DISTRICT COURT

6 DISTRICT OF ARIZONA

7 United States of America,)
8 Plaintiff,) CV-05-457-TUC-DCB
9 v.)
10 Cyberheat, Inc.,)
11 Defendant.)
12 _____)

13 Plaintiff's Motion for Summary Judgment and Defendant's Motion for Partial
14 Summary Judgment are pending before the Court.

15 SUMMARY

16 This action involves enforcement by the Plaintiff Department of Justice,
17 on behalf of the Federal Trade Commission (FTC), of the CAN-SPAM Act (2003)¹ (Act
18 or Statute), and Adult Labeling Rule (Rule) (May 2004), specifically enforcement
19 of the requirement to place warning labels on commercial electronic mail (email)
20 that contains sexually explicit material. 15 U.S.C. §7704 (a) and (d); 16 C.F.R.
21 §316.4. Plaintiff is seeking civil penalties of up to \$11,000 for each violation
22 (Section 5(m)(1)(A) of the FTC Act), a permanent injunction to prevent future
23 violations (Section 13(b) of the FTC Act), and other equitable relief against
24 Defendant.

25 Defendant is an Arizona corporation, Cyberheat, Inc., in the business of
26 offering sexually explicit websites for consenting adults to view by subscription

28 _____)
1Controlling the Assault of Non-Solicited Pornography and Marketing Act of
2003.

1 on the Internet. Cyberheat utilizes a promotional program called TopBucks in
2 which affiliates enter into a contract arrangement with Cyberheat to promote its
3 websites. The affiliate is compensated by Defendant for each successful contact
4 with a Cyberheat website.

5 In a nutshell, Plaintiff alleges that ten of Defendant's affiliates sent
6 a total of 642 sexually explicit, unconsented to, emails in violation of the Act
7 and were paid a total of \$209,120 in commissions within a one year period.
8 During that same time period, Defendant lodged upwards of 400 complaints of
9 computer users who received unwanted sexually explicit emails, with approximately
10 300 of those complaints coming from a single Defendant's affiliate. Plaintiff
11 contends that Defendant did not screen affiliates, supplied affiliates with
12 pornographic promotional materials, did not monitor or oversee its affiliates'
13 promotional activities, and did not readily terminate affiliates after complaints
14 of uninvited sexually explicit spam.

15 Defendant argues that it did not initiate the violative emails, as the
16 Amended Complaint alleges. Defendant contends that it did not intend, nor is
17 there any evidence that Cyberheat intended, that affiliates violate the Statute
18 to promote its website. Defendant further argues that the affiliates acted
19 independently and not as the alter ego of Cyberheat and to find Cyberheat in
20 violation of the Act and the Rule for the acts of these independent affiliates
21 is an overly broad, unintended blanket application of the Statute.

22 PROCEDURAL BACKGROUND

23 On July 20, 2005, Plaintiff filed a Complaint and on August 30, 2005, filed
24 an Amended Complaint for Civil Penalties, Permanent Injunction and Other
25 Equitable Relief. On September 19, 2005, Defendant filed an Answer. On November
26 8, 2005, a Scheduling Order was entered by the Court.

On July 28, 2006, Plaintiff filed a Motion for Summary Judgment (PMSJ), a Memorandum in Support (PMEM), and a Statement of Facts in Support (PSOF). On July 28, 2006, Defendant filed a Motion for Partial Summary Judgment (DMSJ) and a Statement of Facts in Support (DSOF).

On August 28, 2006, Plaintiff filed a Response in Opposition. On August 28, 2006, Defendant filed a Response in Opposition. In addition, Defendant filed an Objection to the Himelfarb Declaration. On September 12, 2006, both parties filed Reply briefs.

Oral argument by the parties was heard by the Court on December 12, 2006. The Court took the matter under advisement and requested the Plaintiff to file a Proposed Permanent Injunction for review. Plaintiff filed a Proposed Permanent Injunction on December 27, 2006. On January 11, 2007, Defendant filed a Memorandum in Response (SuppResp). On January 19, 2007, Plaintiff filed a Reply and a Revised Proposed Permanent Injunction.

DISCUSSION

A. Interpretation of the Statute

"Statutory construction must begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose." *Park 'N Fly, Inc. v. Dollar Park & Fly, Inc.*, 469 U.S. 189, 194 (1985). The Court may consider how a word or phrase is used elsewhere in the same statute, or how it is used in other statutes, *Kungys v. United States*, 485 U.S. 759, 770 (1988), how the possible meanings fit within the statute as a whole, *United States v. Fausto*, 484 U.S. 439, 449-51 (1988), and may rely on the interaction of different statutory schemes to determine statutory plain meaning, so that statutes dealing with similar subjects may be interpreted harmoniously. *Jett v. Dallas Ind. Sch. Dist.*, 491 U.S. 701, 737 (1989).

1 The text of 15 U.S.C. §7704(d)(Statute), reads in pertinent part, as
2 follows:

3 (d) Requirement to place warning labels on commercial electronic
4 mail containing sexually oriented material

5 (1) In general

6 No person may initiate in or affecting interstate commerce the
7 transmission, to a protected computer, of any commercial electronic
8 mail message that includes sexually oriented material and--

9 (A) fail to include in subject heading for the electronic mail
10 message the marks or notices prescribed by the Commission under this
11 subsection; or

12 (B) fail to provide that the matter in the message that is initially
13 viewable to the recipient, when the message is opened by any
14 recipient and absent any further actions by the recipient, includes
15 only--

16 (i) to the extent required or authorized pursuant to paragraph

17 (ii), any such marks or notices;

18 (iii) the information required to be included in the message pursuant
19 to subsection (a)(5) of this section; and

20 (iv) instructions on how to access, or a mechanism to access, the
21 sexually oriented material.

22 The text of the Adult Labeling Rule (Rule), 16 C.F.R. § 316.4, reads as
23 follows:

24 (a) Any person who initiates, to a protected computer, the
25 transmission of a commercial electronic mail message that includes
26 sexually oriented material must:

27 (1) Exclude sexually oriented materials from the subject heading for
28 the electronic mail message and include in the subject heading the
29 phrase "SEXUALLY-EXPLICIT": in capital letters as the first
30 nineteen (19) characters at the beginning of the subject line; ...

31 (2) Provide that the content of the message that is initially
32 viewable by the recipient, when the message is opened by any
33 recipient and absent any further actions by the recipient, include
34 only the following information:

35 (i) The phrase "SEXUALLY-EXPLICIT": in a clear and conspicuous
36 manner; ...

1 (ii) Clear and conspicuous identification that the message is an
2 advertisement or solicitation;

3 (iii) Clear and conspicuous notice of the opportunity of a recipient
4 to decline to receive further commercial electronic mail messages
5 from the sender;

6 (iv) A functioning return electronic mail address or other
7 Internet-based mechanism, clearly and conspicuously displayed, that-

8 (A) A recipient may use to submit, in a manner specified in the message,
9 a reply electronic mail message or other form of Internet-based
10 communication requesting not to receive future commercial electronic mail
11 messages from that sender at the electronic mail address where the message
12 was received; and

13 (B) Remains capable of receiving such messages or communications for no
14 less than 30 days after the transmission of the original message;

15 (v) Clear and conspicuous display of a valid physical postal address of
16 the sender; and

17 (vi) Any needed instructions on how to access, or activate a
18 mechanism to access, the sexually oriented material, preceded by
19 a clear and conspicuous statement that to avoid viewing the
20 sexually oriented material, a recipient should delete the e-mail
21 message without following such instructions.

22 (b) Prior affirmative consent. Paragraph (a) of this section does
23 not apply to the transmission of an electronic mail message if the
24 recipient has given prior affirmative consent to receipt of the
25 message.

26 To violate the Statute, first one must "initiate in or affect interstate
27 commerce." Section 7704. The Statute defines those and other applicable words
28 in Section 7702, as follows:

29 (9) Initiate

30 The term "initiate," when used with respect to a commercial
31 electronic mail message [email], means to originate or transmit such
32 message or to procure the origination or transmission of such
33 message, but shall not include actions that constitute routine
34 conveyance of such message. For purposes of this paragraph, more
35 than one person may be considered to have initiated a message.
36 * * *

37 (12) Procure

38 The term "procure," when used with respect to the initiation of a
39 commercial electronic mail message, means intentionally to pay or
40 provide other consideration to, or induce, another person to
41 initiate such a message on one's behalf.

(16)(A) Sender

* * *

A person who initiates such a message and whose product, service, or Internet website is advertised or promoted by the message.

The *Oxford English Dictionary* (2007) defines "initiate" to "begin, commence, enter upon; to introduce, set going, give rise to, originate, start."

The Senate Report² recommending the Statute for enactment states, with reference to the definition of "initiate," that "more than one person may be considered to have initiated a message, thus, if one company hires another to handle the tasks of composing, addressing, and coordinating the sending of a marketing appeal, both companies could be considered to have initiated the message—one procuring the origination of the message; the other for actually originating it." (S.Rep. 108-102, 2004 U.S.C.C.A.N. 2348.)

Black's Law Dictionary (8th ed. 2004) defines "procure" "as one who induces or prevails upon another to do something, esp. to engage in an illicit sexual act." The *Oxford English Dictionary* defines "procure" as "to try to induce; to urge, press; to induce or prevail upon someone to come; to bring, lead." The Senate Report explains the definition, as follows:

when used with respect to the initiation of a commercial electronic mail message, means intentionally to pay or induce another person to initiate the message on one's behalf, while knowingly or consciously avoiding knowing the extent to which that person intends to comply with this Act. The intent of this definition is to make a company

² "Committee reports are the most frequently cited and relied-upon sources of legislative history, and in the Court's traditional view the most authoritative source. 'A committee report represents the considered and collective understanding of those Congressmen involved in drafting and studying proposed legislation. Floor debates reflect at best the understanding of individual Congressmen. It would take extensive and thoughtful debate to detract from the plain thrust of a committee report ...' Committee reports are often the best evidence of bicameral agreement, either because the House and Senate reports are identical, or because a conference report explicates the chambers' resolution of differences." *2A Sutherland Statutory Construction* § 48A:11 (6th ed.).

1 responsible for an email message that it hires a third party to
2 send, unless that third party engages in renegade behavior that the
3 hiring company did not know about. However, the hiring company
4 cannot avoid responsibility by purposefully remaining ignorant of
the third party's practices. The 'consciously avoid knowing'
portion of this definition is meant to impose a responsibility on a
company hiring an email marketer to inquire and confirm that the
marketer intends to comply with the requirement of this Act.

5 (S.Rep. 108-102. 2004 U.S.C.C.A.N. 2348.).

6 The legislative history leading to the promulgation of the CAN-SPAM
7 Act reveals that:

8 The purposes of this legislation are to: (i) prohibit senders of
9 electronic mail (e-mail) for primarily commercial advertisements or
10 promotional purposes from deceiving intended recipients or Internet
service providers as to the source or subject matter of their e-mail
11 messages; (ii) require such e-mail senders to give recipients an
opportunity to decline to receive future commercial e-mail from them
and to honor such requests; (iii) require senders of unsolicited
12 commercial e-mail (UCE) to also include a valid physical address in
the e-mail message and a clear notice that the message is an
13 advertisement or solicitation; and (iv) prohibit businesses from
knowingly promoting, or permitting the promotion of, their trade or
14 business through e-mail transmitted with false or misleading sender
or routing information.

15 * * *

16 Pornographic spam is more likely than other spam to contain
17 fraudulent or misleading subject lines. In its recent report, the
FTC found that more than 40 percent of all pornographic spam either
18 did not alert recipients to images contained in the message or
contained false subject lines, thus "making it more likely that
recipients would open the messages without knowing that pornographic
19 images will appear." Unsuspecting children who simply open e-mails
with seemingly benign subject lines may be either affronted with
20 pornographic images in the e-mail message itself, or automatically
and instantly taken-without requiring any further action on their
part (like clicking on a link)-to an adult web page exhibiting
21 sexually explicit images.

22 * * *

23 Spam also is used to lure unwary users to websites that contain
viruses, spyware, or other malicious computer code. Late last year,
24 for instance, an Internet adult entertainment company created a
"Trojan horse" program that was downloaded to unsuspecting users
computers. Users were tricked into accepting the program through a
spam message that promised to deliver an electronic greeting card.
The downloaded program, however, instead routed users to the
25 company's pornography websites.

26 * * *

27 Also common is spam with pornographic content or links to websites
with pornographic content, which many recipients find offensive and

which places additional burdens on parents to constantly monitor their children's email.

* * *

Pornographers, long on the cutting edge of technology, have taken to employing increasingly brazen techniques to sell their products and services. As mentioned above, the FTC estimates that 18 percent of all spam is pornographic or "adult-oriented" material. While not all of such spam³ contains images, spammers often do send graphic sexual images embedded in the body of spam so that simply upon opening the e-mail message, a user is assaulted with explicit photographs or video images. More frequently, though, spam contains HTML code and a JavaScript applet that together automatically load a pornographic web page as soon as the spam message is either opened or, in some cases, simply "previewed" in certain e-mail programs preview panes.

⁴ See S. REP. 108-102, 2004 U.S.C.C.A.N. 2348.

In this action, the violative activities of the affiliates and the affiliates' relationship to Cyberheat are the primary issue. Neither the Statute nor the Rule contains the word "affiliate." The *Oxford English Dictionary* defines "affiliate" as "a recognized auxiliary, as an affiliated organization." *Black's Law Dictionary* defines "affiliate" as "a corporation that is related to another corporation by shareholdings or other means of control; a subsidiary, parent, or a sibling corporation; one who controls, is controlled by, or is under common control with an issuer of a security."

Plaintiff's position is that Defendant acted as an initiator, sender and/or procurer, as defined in the Statute, and is directly liable for violations of its affiliates.

Here, Defendant argues that it had no control over the affiliates on how, when, or even if they ever promoted Defendant's website and that the Statute does not apply to this situation. The Terms and Conditions Agreement entered into by

³Spam is unsolicited commercial bulk electronic mail.

⁴SENATE REPORT NO. 108-102 (July 16, 2003, Sen. McCain, Committee on Commerce, Science, and Transportation).

1 affiliates was explicit that violations of the CAN-SPAM Act would not be
2 tolerated and email promotions were not encouraged. Defendant argues that the
3 facts do not support respondeat superior liability or vicarious liability.
4 Defendant further argues that it did not have the ability to monitor or supervise
5 the methods affiliates used to promote their website. "Since Cyberheat did not
6 authorize its affiliates to use its promotional materials in emails, and since
7 Cyberheat did not authorize its affiliates to send emails on Cyberheat's behalf,
8 and since nothing in the contractual relationship provided the affiliates the
9 power to do either on behalf of Cyberheat, the only remaining possibility for
10 extending liability to Cyberheat for the acts of the affiliates is if the
11 affiliates had the apparent authority to send the emails on Cyberheat's behalf."
12 (SuppResp at 5.)

13 The text of the Statute plainly contemplates a situation where one entity
14 or person either pays for or otherwise induces another person or entity on their
15 behalf to send a violative email such that a joint violation of the Statute has
16 occurred. The Statute states specifically that more than one person may be
17 considered to have initiated a particular message. The text also makes it clear
18 that procuring involves somehow inducing, either by money or otherwise, as part
19 of the initiation of the particular message.

20 The CAN-SPAM Act was not enacted in a vacuum. Congress was compelled to
21 enact a Statute to protect the Internet-using public from uninvited, unwanted
22 sexually explicit email "by imposing limitations and penalties on the
23 transmission of unsolicited commercial electronic mail via the Internet," because
24 "[u]nsolicited commercial email, commonly known as spam, has quickly become one
25 of the most pervasive intrusions in the lives of Americans."⁵ A portion of that
26 Statute deals specifically with sexually explicit materials otherwise known as

27
28 ⁵S. Rep. 108-102, 2004 U.S.C.C.A.N. 2348.

1 pornography. What precipitated the focus on pornography was not the availability
2 of pornography to consenting adults, but the unexpected, uninvited pornographic
3 spam email messages that appear with no warning in plain view of anyone using the
4 Internet at the time, from a nine-year-old student studying for a history test
5 to an 80-year-old great aunt looking to send a greeting card. The Statute
6 creates a legal obligation, a duty, assigned to those who are in the business of
7 sending sexually explicit materials over the Internet. The duty is owed to the
8 public, particularly those members of the public who use the Internet but do not
9 consent to view sexually explicit materials. Reasonable care must be taken to
10 ensure that those members of the public who do not chose to view sexually
11 explicit materials on the Internet are not involuntarily subjected to those
12 materials. The Act and the Rule are very specific about the reasonable care
13 required to prevent uninvited pornographic Internet intrusions. It is foreseeable
14 that when sexually explicit promotional materials are supplied to third parties,
15 violations of the Act and Rule may occur. A duty of care arises when it is
16 foreseeable that harm may result if care is not exercised. See, e.g., *Salinas*
17 v. United States, 9 Fed. Appx. 662 (9th Cir. 2001). It is foreseeable that harm
18 may result if care is not exercised here, particularly because of the nexus
19 between the third party violations and the sexually explicit promotional
20 materials provided by the company. The doctrine of vicarious liability applies
21 to the enforcement of this portion of the Statute, because of the burden of the
22 duty imposed on the provider of pornography on the Internet. Vicarious liability
23 is the exception to the normal principal of individualized fault. It is
24 liability imposed on one person for the harm caused by another because the duty
25 is so important that is it not delegable or delegable at the peril of the duty
26 holder. Further, the regulation of sexually explicit spam is unique and
27 distinguishable from fraudulent or misrepresentative materials regulated by the
28

Act. To experience the violation derived from fraud and misrepresentation contained in an unsolicited email message requires review and consideration of the content, unlike the viewing of uninvited, unsolicited pornography which results in immediate harm.

The Statute directly applies to Cyberheat, as a provider of sexually explicit materials⁶ for viewing on the Internet. Cyberheat maintains that a strict liability approach is not what the Statute contemplates and the Court agrees, for now. Cyberheat is a business and the Court will balance Cyberheat's economic needs (burden of the duty) with the need to enforce the Statute for the benefit of the public (foreseeability of the harm). Here, the Court does not find the Statute applicable to a business such as Cyberheat for an accidental or mistaken violation, immediately attended to and corrected. By the same token, Cyberheat cannot insulate itself from any liability for the actions of the affiliates on its ultimate behalf and for its financial benefit purely by putting on blinders or inattention to monitoring and supervising the use of its sexually explicit materials.⁷ Cyberheat has a duty that it can only delegate at its own peril. In the end, Cyberheat is paying affiliates who are successful in promoting Cyberheat and bringing in business to the company. Because Defendant is a purveyor of that which the Statute explicitly attempts to regulate, sexually explicit materials available on the Internet, the Court does view Defendant as having a duty to oversee the use of those sexually explicit materials when distributed for promotion, and despite the disclaimers, upon receipt of knowledge

⁶Plaintiff supplied the Court with examples of the violative sexually explicit emails in question and it would be fair to say that these emails consist of full page (top to bottom) pornography that leaves nothing to the imagination.

⁷In a case involving imputed negligence, liability will be imposed on one person for the negligence of another based on the relationship between the parties, or arising from a rule of statutory law, or contract...Essentially the negligence of one person will not be imputed to another unless there exists a legal obligation to respond to the other's fault. 57B *Am.Jur. 2d Negligence* §1096.

1 that affiliates were using their promotional literature in a violative manner,
 2 incurred a duty to act reasonably to stop that activity. Here, control over the
 3 affiliates and knowledge of the violations of the affiliates are two issues that
 4 are pivotal.⁸

5 In sum, the Court finds that the Act and Rule apply to the relationship
 6 between Cyberheat and its affiliates, such that the company may be held
 7 vicariously liable for the actions of the affiliates⁹, depending on a resolution
 8 of the facts concerning control and knowledge.

9 **B. Dispositive Motions**

10 **1. Legal Standard**

11 Summary judgment is proper "if the pleadings, depositions, answers to
 12 interrogatories, and admissions on file, together with the affidavits, if any,
 13 show that there is no genuine issue as to any material fact and that the moving
 14 party is entitled to a judgment as a matter of law." Fed.R.Civ.P. 56(c)). The
 15 moving party bears the initial burden of demonstrating the absence of a genuine
 16 issue of material fact. See *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986).
 17 The moving party, however, has no burden to negate or disprove matters on which
 18 the non-moving party will have the burden of proof at trial. The moving party
 19 need only point out to the Court that there is an absence of evidence to support
 20 the non-moving party's case. See *id.* at 325.

21

22 ⁸Other enforcement statutes enacted to protect the public have been applied
 23 based on the principles of vicarious liability: *Fare Deals Ltd. v. World Choice*
Travel.Com, Inc., 180 F.Supp.2d 678 (D.Md. 2001)(AntiCybersquatting/vicarious
 24 liability); *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259 (9th Cir.
 1996)(copyright and trademark infringement/vicarious liability); and, *Hard Rock*
Cafe Licensing v. Concession Services, Inc., 955 F.2d 1143 (7th Cir. 1992)(Lanham
 25 Trademark Act/vicarious liability). These cases involve a resolution of facts
 concerning control and knowledge.

26 ⁹The doctrine of vicarious liability is based on the relationship between
 27 the parties, whereby it is deemed a matter of public or social policy that
 regardless of fault one party should be liable for the acts of the other. 57B
 28 Am.Jur. 2d Negligence §1097.

1 The burden then shifts to the non-moving party to "designate 'specific
2 facts showing that there is a genuine issue for trial.'" ' See *Celotex Corp.*, 477
3 U.S. at 324 (quoting Fed.R.Civ.P. 56(e)). To carry this burden, the non-moving
4 party must "do more than simply show that there is some metaphysical doubt as to
5 the material facts." *Matsushita Elec. Indus. Co., Ltd. v. Zenith Radio Corp.*, 475
6 U.S. 574, 586 (1986). "The mere existence of a scintilla of evidence . . . will
7 be insufficient; there must be evidence on which the jury could reasonably find
8 for the [non-moving party]." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 252
9 (1986). In a motion for summary judgment, the evidence is viewed in the light
10 most favorable to the non-moving party, and all justifiable inferences are to be
11 drawn in its favor. See *id.* at 255. "Credibility determinations, the weighing of
12 the evidence, and the drawing of legitimate inferences from the facts are jury
13 functions, not those of a judge . . . ruling on a motion for summary judgment."
14 *Id.*

15 2. Plaintiff's Case

16 After a thorough and extensive investigation conducted by investigators at
17 the FTC, Plaintiff filed an civil enforcement action against Cyberheat pursuant
18 to 15 U.S.C. §7704 (a), (d) and 16 C.F.R. §316.4. In Count I, Plaintiff claims
19 that Defendant's acts and practices violate 15 U.S.C. §7704(d) and 16 C.F.R.
20 §316.4(a) by initiating transmissions of commercial email messages to protected
21 computers that include sexually oriented material and fail to include the phrase
22 "sexually-explicit" within the first nineteen characters; fail to include within
23 the initially viewable content message, "sexually-explicit"; fail to include
24 notice and opportunity to decline; fail to include physical postal address of
25 Defendant; and include sexually oriented material within the initially viewable
26 content of the message. In Count II, Plaintiff alleges that Defendant initiated
27 these transmissions with email messages that advertised or promoted Defendant's
28

1 Internet web sites without the requisite notice or opportunity to decline. Count
2 III alleges that same as above but that the messages failed to include
3 Defendant's valid physical postal address.

4 The government contends that there are no material questions of fact
5 precluding resolution of the dispositive motion and that Defendant may be found
6 in violation of the Act and Rule based on the actions of its affiliates. The
7 primary document in support of Plaintiff's case is the Allyson Himelfarb
8 Declaration. Her Declaration is supported by attached documents which were filed
9 electronically and are contained on a CD-ROM disc.

10 Himelfarb is an investigator with the FTC in the Division of Marketing
11 Practices, Bureau of Consumer Protection. Her job is specifically to investigate
12 persons/entities who may be violating the Act and Rule, and to do so she
13 utilizes Internet search engines, electronic databases and a variety of other
14 computer-based investigative tools. Himelfarb's Declaration and the attachments
15 are intended to show conclusively the Cyberheat and the affiliates were
16 connected, as well as Cyberheat's knowledge of its affiliates' activities.

17 Himelfarb began investigating Defendant, identified as an operator of an
18 online affiliate program called TopBucks that promotes and advertises dozens of
19 adult entertainment websites, in December 2004. The investigation was initiated
20 when Cyberheat was identified as an adult website that was allegedly violating
21 the Act and the Rule thorough email message promotions. These messages were
22 identified by the FTC's spam database, as well as the "Hotmail trap accounts"
23 maintained by Microsoft Corporation. Himelfarb's job was to peel away the layers
24 to generally identify: the company that owned or registered the adult website
25 promoted by the messages; where possible, the individual entity that physically
26 sent the email messages (affiliate); how many different affiliates sent emails

1 on Cyberheat's behalf; how many emails each affiliate sent; and, the number of
2 recipients to which the emails were sent.

3 Himelfarb reviewed the identified emails for specific violations: (1) was
4 the phrase "sexually-explicit" in the subject line and initially viewable area
5 of the message; (2) was there sexually explicit text or images within the
6 initially viewable area of the message; (3) was there a notice to opt-out within
7 the viewable area; and (4) was there a valid physical postal address for
8 Cyberheat within the initially-viewable area. Microsoft responded to the FTC's
9 requests for information about Cyberheat email messages caught in its Hotmail
10 trap accounts. To identify each email message provided by Microsoft, it provided
11 two files: one file in Internet email format, ".eml" and one file in a portable
12 document format, ".pdf". The .eml files reflect the source code and the .pdf
13 files preserve the content of the email messages. To peel away the layers,
14 Himelfarb:

15 [R]eviewed the source code of the .eml files in order to
16 identify the Uniform Resource Locators or URLs contained in the
17 email messages. The URL is a unique address of a specific file or
18 webpage on the Internet. A URL is comprised of the name of the
19 protocol to be used to access the file (commonly called HTTP), a
20 domain name that identifies a specific computer on the Internet and
21 a pathname, a hierarchical description that specific location of the
22 file on the computer. In the emails that [Himelfarb] reviewed,
23 typically one URL identified the hyperlink that the recipient would
click to access the adult website being promoted by the email
message. This URL is commonly referred to as the hyperlink
reference and is typically signified by the identified in an email
message's source code. Microsoft used these hyperlink reference
URLs to perform "web captures." The web captures preserved the web
page that a user would be directed to upon clicking the hyperlink
reference URL.

24 (PMSJMem, Ex. 1 at 3.)

25 If the .pdf contained sexually explicit material, then Himelfarb checked
26 to see whether the email violated the Act and the Rule. She then used the .eml
27 to identify the source code for the message. She used Microsoft's web capture

1 to trace the website as registered to Cyberheat. The Microsoft web capture also
2 identified the affiliate with an affiliate ID assigned to the affiliate by
3 Cyberheat, in order for her to connect that affiliate's activity back to
4 Cyberheat.

5 Some identified emails were not captured by Microsoft. In that case,
6 Himelfarb clicked on the hyperlink contained in the email message and preserved
7 the web page or pages to which the hyperlinks redirected. Himelfarb reviewed
8 hundreds of email messages sent by 10 of Cyberheat's affiliates. The results of
9 these emails were saved either in .pdf or .eml formats, as well as in HTML format
10 for certain messages, along with related web captures and other recordings on a
11 CD-ROM filed with the Court. During discovery Cyberheat also produced a list of
12 domain names and payment information.¹⁰

13 The Plaintiff's position is that money in the form of commissions to
14 affiliates and profit in the form of new business to Cyberheat was the motive for
15 the use of violative emails to promote Cyberheat's website. "Affiliates of the
16 Topbucks program are paid to advertise Cyberheat's websites, earning money each
17 time they refer a customer who subscribes to one of the Cyberheat's adult
18 websites." (PSOF at 3.) In effect, affiliates that participated in the TopBuck
19 program were paid a commission for traffic and sales to Cyberheat.

20 Plaintiff contends that there is sufficient evidence to find Cyberheat
21 aware of and directly responsible for these violations. Plaintiff lists the
22 following: Cyberheat's screening process for affiliates was not significant; it
23 had a policy not to approve an affiliate application previously determined to be
24 a cheater or spammer, yet it did not ask affiliates if they intended use email
25 to promote; it assigned affiliates with a unique four or five digit number to

27 ¹⁰Himelfarb's Declaration goes on to, in explicit detail, explain the
28 layers connecting the violating affiliate emails to Cyberheat.

1 track sales and to determine payment as commission for sales; some entities had
2 more than one affiliate account with Cyberheat; the company provided free
3 webhosting, marketing and promotional tools to affiliates - all featuring the
4 sexually explicit material available on the Cyberheat website; and, affiliates
5 had the ability add a hyperlink to the promotional materials and use them in
6 emails, so that when pressed, these hyperlinks went directly to the Cyberheat
7 sexually explicit website being advertised. Cyberheat provided affiliates with
8 hourly statistics on the number of sales and clicks they have generated, as well
9 as 24 hour assistance in some form to affiliates.

10 The Plaintiff asserts that Cyberheat was aware that email was a source of
11 promotion and that affiliates had the potential to send unlawful spam as a means
12 to advertise Cyberheat. Cyberheat had a method to receive and review complaints
13 about unwanted spam. Complaints were forwarded to a spam complaint email
14 account. "Between May 14, 2004 and June 7, 2005, Cyberheat received over 400
15 complaints from individuals who received unwanted commercial email messages from
16 Cyberheat affiliates promoting Cyberheat's websites." (PSOF at 8.) Cyberheat
17 did not terminate every affiliate who was the subject of a complaint and in some
18 cases, reinstated previously terminated affiliates. If one of an affiliate's
19 accounts was terminated for violations, not all of that affiliate's accounts were
20 terminated. Cyberheat's Terms and Conditions for affiliates stated that
21 affiliates should not use or employ any form of mass unsolicited electronic
22 mailings and had an informal unwritten policy that affiliates should not
23 advertise by email. Cyberheat did not employ any of the monitoring methods that
24 were identified in this informal policy which was only disclosed to a handful of
25 affiliates. Cyberheat relied on the provisions in the Terms and Conditions to
26 prevent violations, as well as the reservation to terminate affiliates who
27 violated the law.

1 Plaintiff contends the Defendant misconstrues the knowledge/intent element
2 of the Statute. "The Act does not require any showing of specific intent or
3 knowledge for liability to attach. Rather, Cyberheat's procurement of violative
4 emails makes Cyberheat liable for injunctive relief for violating the Act.
5 Furthermore, while not necessary for injunctive relief, Cyberheat's actual or
6 constructive knowledge of the violations was sufficient to make it liable for
7 civil penalties." (PResp at 11.) "What is required to find Cyberheat liable
8 under the Act is something less than actual knowledge that its affiliates are
9 engaging, or will engage, in a pattern or practice that violates this Act. That
10 knowledge may be required for a criminal violation, but this is not a criminal
11 case. What is required is less than consciously avoiding knowing that its
12 affiliates are engaging in, or will engage, in a pattern of practice that
13 violates the Act." (Id., 17-18.) Plaintiff does not have to prove conscious
14 avoidance, just that the violations did not occur by accident. According to
15 Plaintiff, "Congressional intent to impose liability in FTC enforcement actions
16 against those who cause CAN-SPAM violations, regardless of their "knowledge of
17 the violations, could hardly be clearer." (PResp at 14.) "Cyberheat's agreement
18 with affiliates to provide advertising services foreseeably involved the
19 affiliates/ use of on-line advertising including email. Cyberheat even knew that
20 some of its affiliates were using spam to promote Cyberheat's websites." (PResp
21 at 19.) "Cyberheat argues that for liability to attach the Act requires that
22 Cyberheat paid its affiliates." (Id.) Defendant admits that it entered into
23 agreements with the third parties whereby it paid those third parties a
24 commission or finders fee for sales resulting from referrals by those third
25 parties to Defendant's Web sites." (PResp at 11.) "Defendant attempts to draw
26 a distinction between this practice and paying the third parties to market or
27 advertise Defendant's websites. Defendant does not disagree with the Government
28

1 concerning the facts surrounding the relationship between Cyberheat and its
 2 affiliates, it merely argues that those facts do not make Cyberheat liable for
 3 the violations." (PResp at 11.)

4 3. Cyberheat's Defense

5 Defendant denies that it was an initiator, procurer or sender in violation
 6 of the Act. It also denies that it is in violation of the Act through the
 7 actions of its affiliates, who Defendant claims in turn have violated their
 8 agreements with Defendant by violating the law.¹¹

9 Defendant argues that there are questions of fact precluding summary
 10 judgment in Plaintiff's favor: whether payment before the transmission of the
 11 violating email was required to show a violation of the Act; whether defendant
 12 actually allowed its affiliates to use its marketing tools in illegal emails,
 13 reflecting direct evidence of knowledge/intent; whether any terminated
 14 affiliates were ever reinstated; whether it was feasible for Defendant to monitor
 15 the activities of its affiliates¹²; and, whether there was affirmative consent
 16 to 21 of the purportedly violative emails.¹³

17 The true bone of contention comes when Defendant begins to argue its case
 18 that they should not be held responsible for the emails sent by the affiliates,
 19 also called the independent "Webmasters" by the Defendant. The contract between
 20 TopBucks, Cyberheat's promotional entity, and the third parties is called the
 21

22 ¹¹The first eleven pages of Defendant's dispositive motion goes to emails
 23 sent by Defendant to persons who consented to acceptance of the emails. The
 24 Plaintiff agrees that none of those emails are violations of the Statute and were
 25 never part of the Amended Complaint. The only violative emails in question are
 26 the ones sent by Cyberheat's affiliates.

27 ¹²Defendant's objection to the submission of the Himelfarb Declaration is
 28 overruled. It is not submitted as an expert opinion but merely a compilation of
 29 the results of an investigation.

30 ¹³For purposes of this motion, Plaintiff waived those emails in lieu of
 31 pursuing this action on the remaining 600 or so at issue.

1 Terms and Conditions Agreement and specifically refers to the third parties as
2 affiliates. Defendant's primary argument is that the "Defendant did not
3 actually send these emails." (DMPSJ at 11.) In addition, the third parties were
4 not paid to send the emails to promote Cyberheat's websites, rather were paid a
5 "finders fee if, and only if, someone whom the third party had referred to one
6 of Defendant's websites subsequently subscribes to the website." (Id.)
7 Defendant further argues that "the critical point that the Court must understand
8 is that Defendant never expressly, implicitly or otherwise authorized such person
9 to violate the CAN-SPAM." (Id.) Defendant relies on the fact that the Terms and
10 Conditions specifically forbids affiliates to violate the CAN-SPAM Act.

11 Defendant's express position is that as long as Defendant did not permit
12 or condone the illegal activity, Defendant cannot be held liable under the Act.
13 The egregious emails were sent by third parties who "were not the Defendant or
14 the Defendant's employees, officers, directors or shareholders." (Id. at 13.)
15 Defendant denies that it initiated, induced or procured the violative emails, as
16 defined by the Statute. Defendant denies that it is liable under the "pay or
17 provide" definition. Defendant insinuates that the Statute requires intent for
18 Defendant to be held liable for the acts of the third parties and there is no
19 direct evidence of intent in the record. "Defendant must have intentionally paid
20 or provided compensation to another to send the illegal email or it must have
21 intentionally induced another to do so." (Id. at 19.) Defendant goes on to argue
22 that Plaintiff is applying a strict liability analysis to include Defendant as
23 a violator for third party acts.

24 Cyberheat treats and describes the affiliates as more like independent
25 contractors, persons who perform services for another person under an express or
26 implied agreement and who are not subject to the other's control or right to
27 control the manner or means of performing the services, than agents, acting
28

1 within the scope of authority in the performance of duties which are expressly
2 or impliedly assigned by the principal. There are no facts to suggest that
3 Cyberheat was violating the Act but for the use of the affiliate promotional
4 program. There are also no facts that Cyberheat directed affiliates to promote
5 its website by violating the Statute. Cyberheat did not direct affiliates to
6 utilize the promotional materials in emails and possibly had an informal
7 arrangement that emails would not be used at all.

8 Cyberheat also raises questions that suggest that due to the
9 infinitesimally small number of affiliates who used violative email messages, the
10 question of knowledge and duty on the part of Cyberheat is particularly relevant.
11 Plaintiff has focused on 12 Cyberheat Webmasters out of upwards of 50,000
12 affiliates of which only about 10,000 successfully referred subscribers, or 2/100
13 of one-percent of the registered affiliates utilized email to promote. (SuppResp
14 at 11.) Cyberheat argues that the government's proposed permanent injunction,
15 in light of the facts here, is overbroad and onerous.

16 The Defendant contends that it cannot be found in violation of the Act
17 because it did not intentionally induce the violative email messages or
18 intentionally induce its affiliates to send the violative email messages.
19 Defendant asserts that it had no control over the actions of its affiliates.
20 Defendant argues that it did not know about or consent to the violations.

21 4. Control

22 Cyberheat's ability to control, monitor and supervise affiliates is a fact
23 question. Cyberheat claims to utilize affiliates on an independent basis with
24 no control over methodology other than the Terms and Conditions Agreement.
25 Cyberheat does not monitor or oversee the actions of affiliates other than
26 accounting for business referred to Cyberheat by an affiliates for which they are
27 compensated. Cyberheat does not direct the promotional activities of the
28

1 affiliates, yet they do provide promotional materials. Factually, Cyberheat and
2 its affiliates appear distant and removed, other than some nominal support. The
3 terms of the affiliate agreement evince no intent on the part of Cyberheat or any
4 of the affiliates to enter into a principal-agent relationship.

5 Yet, based on the duty imposed by this Act, if Cyberheat is not a direct
6 violator of the Statute, it may be vicariously liable for the foreseeable
7 violations of its affiliates. The law of agency, in appropriate circumstances,
8 renders a principal vicariously liable for the torts of its agent. *Am. Soc. of*
9 *Mech. Eng. v. Hydrolevel Corp.*, 456 U.S. 556, 565-66 (1982). A court may apply
10 traditional rules of agency law to a federal statute's civil liability provision
11 when those rules accord with the statute's purpose and when Congress has not
12 indicated otherwise. *Thomas v. Ross & Hardies*, 9 F.Supp.2d 547, 557
13 (D.Md.1998). For example, Courts have reasoned that because the Lanham Act's
14 purpose of prohibiting unfair competition would go largely unrealized if it
15 absolved principals from the trademark-infringing acts of their agents, and
16 because the Act itself does not disavow such liability, a cause of action under
17 the Lanham Act may lie vicariously against a principal. See *Am. Tel. & Tel. Co.*
18 *v. Winback & Conserve Program, Inc.*, 42 F.3d 1421, 1437 (3d Cir.1994).

19 "Agency is the fiduciary relation which results from the manifestation of
20 consent by one person to another that the other shall act on his behalf and
21 subject to his control, and consent by the other so to act." Rest. 2d Agen. §

22 1. The creation of an agency relationship ultimately turns on the parties'
23 intentions as demonstrated either by express agreement or by inference from their
24 actions. *Fare Deals, Ltd.*, 180 F.Supp.2d at 685 (operator of web site which was
25 advertised on and hyperlinked to allegedly trademark infringing web site could
26 not be held vicariously liable for false designation of origin or dilution;
27 operator provided no support for and had no authority to control allegedly
28

1 infringing web site, and lacked knowledge of alleged infringement.) Courts
2 examine three factors in determining whether a principal-agent relationship
3 exists: first, the principal's right to control the alleged agent; second, the
4 alleged agent's duty to act primarily for the benefit of the principal; and,
5 third, the alleged agent's power to alter the legal relations of the principal.

6 *Id.* These factors provide guidance, but "[t]hey are neither exclusive nor
7 conclusive considerations." *Id.* The parties' intent controls, and a court must
8 ascertain their intent "within the context of the entire circumstances of the
9 transaction or relations." *Id.* The question of agency is a factual matter,
10 and, if any legally sufficient evidence of an agency relationship is produced,
11 it must be submitted to the fact-finder. *Id.* The substance of the parties'
12 relationship, not the label they give it, determines the existence of agency.
13 *Cerniglia v. Pretty*, 674 F.Supp. 1167, 1170 (D.Md.1987).

14 A principal will be held liable for an independent contractor or agent's
15 wrongdoing "upon matters which the principal might reasonably expect would be the
16 subject of representations, provided the other party has no notice that the
17 representations are unauthorized." *Rest. 2d Agen.* §258. Vicarious liability is
18 indirect legal responsibility. It is the attribution of a wrongdoer's actions to
19 an innocent third party by virtue of their relationship. Under common-law tort
20 rules, a joint tortfeasor may bear vicarious liability for the violations of
21 others. Joint tortfeasors are those either in apparent or actual partnership, or
22 with authority to bind each other in transactions with third parties, or with the
23 ability to exercise joint ownership or control over the violator. 57B *Am. Jur.2d*
24 *Negligence* §1096; see *Hard Rock Café*, 955 F.2d at 1149; see also *Rest.2d Agen.*
25 §§ 261, 262.

26 In finding vicarious liability, too, the relationship between the defendant
27 and the alleged violator is very significant. For a parent to be held secondarily
28

1 liable for its subsidiary's acts, there must be a sufficient link between them.
2 In *Banff Ltd. v. Limited, Inc.*, 869 F. Supp. 1103 (S.D.N.Y. 1994), a corporate
3 parent was held not vicariously liable for its subsidiary's trademark
4 infringements where the parent made no decisions regarding sales and purchases
5 and had no involvement in operating any of the subsidiary's retail stores, and
6 where the two had different headquarters, kept separate financial records, and
7 filed separate tax returns. In *Am. Tel. & Tel. Co.*, 42 F.3d at 1437, the court
8 held that a telecommunications company, offering users access to the plaintiff's
9 network at discounted prices, would be vicariously liable under the Lanham Act
10 for its sales representatives' overtly stating or misleading customers to believe
11 that its programs were affiliated with the plaintiff if those actions were
12 foreseeable and the customers had no notice that the representations were
13 unauthorized. That court applied basic principal and agent law and concluded that
14 when a principal authorizes its independent contractor or agent to conduct and
15 conclude a transaction with third parties on the principal's own behalf, and the
16 principal benefits financially from the contracts, the principal will be liable,
17 based on the agents' foreseeable infringing actions upon which it would be
18 reasonable for the third party to rely, provided the third party has no notice
19 that the representations are unauthorized. In *Mini Maid Services Co. v. Maid*
20 *Brigade Systems, Inc.*, 967 F.2d 1516 (11th Cir. 1992), the court held that a
21 franchiser may not be held vicariously liable for one of its franchisees'
22 trademark infringements. Since, it held, the law imposes no duty upon a
23 franchiser to exercise reasonable diligence to prevent independent acts of
24 trademark infringement by franchisees, this defendant was not liable for its
25 franchisees' enjoying the benefits of a yellow pages listing from one of the
26 plaintiff's franchisees after having purchased the phone number from the latter.
27
28

1 A factual question is raised by both parties concerning how much power and
2 ability Cyberheat had to control, monitor or supervise affiliate operations and
3 whether the company acted reasonably under the circumstances.

4 5. Knowledge

5 Further of concern is the question of Defendant's alleged knowledge of
6 violations and inaction to stop violations. Defendant contends that it did not
7 know about or consent to the violations.

8 Notice of the violations to Defendant and whether Defendant's response to
9 the notice of the affiliates' violations was reasonable under the circumstances
10 is a fact question. *See Perfect 10, Inc. v. CCBill, LLC*, 340 F.Supp. 2d 1077
11 (C.D. Cal. 2004). Under the Statute, Cyberheat as a company that offers sexually
12 explicit materials to consenting adults over the Internet, by using affiliates
13 to promote and bring in business. Cyberheat provided sexually explicit materials
14 to affiliates to promote its website. Foreseeably, affiliates could violate the
15 Statute and Rule by utilizing email with sexually explicit materials to promote
16 the website. The Terms and Conditions Agreement appears to sufficiently warn the
17 affiliates of what Cyberheat will and will not tolerate.

18 Although, Plaintiff's investigation reflects that Cyberheat received
19 information that the affiliates were violating the Statute and then did not
20 follow their own promise to terminate violating affiliates. The examples
21 resulting from Plaintiff's investigation are, as follows: Affiliate 28487 who
22 sent four unsolicited violative commercial email messages in August 2004, but not
23 terminated until October 2005; Affiliate 28426 who sent one unsolicited violative
24 commercial email message in August 2004, but has never been terminated;
25 Affiliate 11604 who sent 45 violative messages in August 2004 and has not been
26 terminated; Affiliate 36828 who sent 26 violative messages and is an active
27 account; Affiliate 26377 who sent 1 unsolicited message and is still an active
28

1 account; Affiliate 38485 who sent 4 messages and is an active account; Affiliate
2 43717 who sent five unsolicited messages and is still an active account; and, the
3 list goes on. According to Plaintiff, Cyberheat has a pattern of receiving
4 complaints of violative emails, but not responding at all or belatedly
5 responding, then possibly reinstating violating affiliates. Plaintiff claims
6 that Defendant turned a blind eye to violating affiliates even after they were
7 made aware of the violations. Defendants claim that they acted properly and
8 promptly, under the circumstances.

9 Generally, whether the breach or violation of a statute has occurred, and
10 whether that breach or violation was without valid excuse is a question of fact
11 for a jury. 65A C.J.S. Negligence §842 (2006). Where conflicting evidence is
12 introduced as to any one of the elements necessary to constitute the violation
13 of a statute, a jury question is created, such that it is within the jury's
14 province to assess the credibility of witnesses and determine whose testimony and
15 evidence warrants belief. *Id.*; see *America Online, Inc. v. National Health Care*
16 *Discount, Inc.*, 174 F.Supp. 2d 890 (N.D. Iowa 2001).

17 **CONCLUSION**

18 Here, overall, the evidence produced by both parties raises material
19 questions of fact regarding the relationship between Cyberheat and its
20 affiliates. These material questions of fact go to the heart of the relationship
21 between Cyberheat and its affiliates, specifically what if any control or
22 supervision Cyberheat exerted or could or should have exerted over affiliates
23 based on the content of the promotional materials provided. The material
24 questions of fact also go to the knowledge Cyberheat acquired that affiliate
25 violations were occurring, as well as what actions Cyberheat took upon receiving
26 knowledge of violations and whether its actions were reasonable under the
27 circumstances.

1 Plaintiff argues that these questions involve undisputed facts, but that
2 is not the case, because the evidence is circumstantial, disputed and requires
3 credibility assessments. Reasonable jurors could differ over whether or not
4 Defendant was knowingly procuring or should have known or was consciously
5 avoiding knowing that affiliates were violating the Statute to promote
6 Defendant's website. Plaintiff's evidence concerning Cyberheat's relationship
7 with affiliates is circumstantial and requires the Court to draw factual
8 inferences and make credibility determinations that preclude resolution by
9 summary judgment. Defendant has raised more than some metaphysical doubt as to
10 the material facts. *Matsushita Elec. Indus. Co.*, 475 U.S. at 586. The court
11 recognizes its obligation to view all facts in a light most favorable to the non-
12 moving party and finds that a reasonable trier of fact could differ over whether
13 or not that the relationship between Cyberheat and its affiliates resulted in
14 vicarious liability for violations of the Statute.

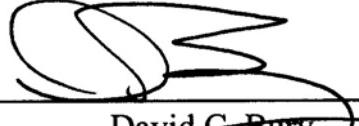
15 A trier of fact may consider the complaints about the affiliates' violative
16 activities to the company and Cyberheat's response to those complaints in
17 reaching a conclusion. These particular facts may result in civil penalties of
18 up to \$11,000 per violative email. *Tull v. United States*, 481 U.S. 412 (1987).

19 Accordingly,

20 IT IS ORDERED that Plaintiff's Motion for Summary Judgment (Doc. No. 24)
21 and Defendant's Motion for Partial Summary Judgment (Doc. No. 28) are DENIED.

22 IT IS FURTHER ORDERED that the parties should submit a joint proposed
23 pretrial order on April 27, 2007. A pretrial conference will be set upon receipt
24 of the pretrial order and a trial date will be set at the pretrial conference.

25 DATED this 2nd day of March, 2007.

26
27
28


David C. Bury
United States District Judge

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28